ANALYSIS OF E-WALLET APPLICATIONS FOR PRIVACY AND SECURE DATA USING MODERN COMPUTING PARADIGMS

Dr. K.S. Mohanasathiya
Associate Professor, School of Computer Science,
VET Institute of Arts and Science (Co-Edu) College, Erode, Tamil Nadu, India.
{sathyaanandh08@gmail.com}
Dr. S. Prasath
Assistant Professor, School of Computer Science,
VET Institute of Arts and Science (Co-Edu) College, Erode, Tamil Nadu, India.
{softprasaths@gmail.com}
Dr. K. R. Ananth
Associate Professor & Head, School of Computer Science,
VET Institute of Arts and Science (Co-Edu) College, Erode, Tamil Nadu, India.
{kranand@vetias.ac.in}

Abstract - ***Due to the development of the Internet of Things (IoT), people are surrounded by millions of smart devices to gather massive amounts of data. Internet of Things (IoT) smart devices are more familiar and have more processing capacity, whereas vast volumes of data are processed at the edge of computing networks. Data from IoT devices have traditionally been relayed to a central network server housed in a datacentre. Edge computing is a modern computing paradigm in which data is stored at a neighboring edge node with adequate resources to meet device requirements and improve user knowledge. In this work, while providing data to an edge node, maintaining privacy and security is a difficult and a challenging task. As a result, encrypted data are required to be safeguarded from security attacks. In this phase, an attribute-based conjunctive keyword search method is utilized in conjunction with a proxy re-encryption technique to protect user data in the cloud. This makes it easier for the owner to encrypt data using a private key and the user to search for documents using conjunctive keywords. After the data has been re-encrypted with a new key, only authenticated users can obtain the required documents. In this phase, designed to track previously searched records in order to minimize search time and enhance search computational overhead. The proposed scheme uses time sealer to guarantee the allocated time to every user in the cloud server and great privacy in the cloud is accomplished with efficiency. The proposed scheme gives better results when compared with existing Time Domain Multi-Authority Outsourcing (TMO) and Online/Offline Multi-Authority Decryption Outsourcing (OOMADO) methods in data security.***

Keywords: IOT, OOMADO, TMO, SSE, PEKS

I. Introduction

Internet of Things (IoT) devices grow more and have more processing capacity, massive amount of data is created at the "edge" of computer networks. Traditionally, data from IoT devices have been routed to a centralized network server, which is generally located in a data centre. By relocating critical data processing towards the network edge, edge computing solves this latency problem. Edge enabled devices gather and analyze data in real time, instead of continually sending data back to the central server, allowing them to respond quicker and more efficiently. Edge computing is a flexible approach to network infrastructure which takes advantage of the enormous processing power provided by the combination of modern IoT devices as well as edge datacentres and can be used in conjunction with edge datacentres.

Edge Computing has evolved as a new computing platform where data is handled at the closest edge node with sufficient capabilities to meet application needs and improve user interface [6]. Edge computing has two distinct advantages over cloud computing. To begin, it makes advantage of available computing and storage resources on edge devices located near consumers to enhance response times. Secondly, because bulk data do not have to be sent to the cloud, the mainline bandwidth is conserved. In edge servers and IoT applications, data security and privacy management pose significant problems. Edge computing can move some storage and computation task activities from cloud computing environment to the networks edge, which might pose a number of security and privacy issues. [3]

The phrase "searchable encryption" refers to the ability to examine encrypted data on an unsecured server or cloud without having to decrypt it. This research work uses an attribute-based conjunctive keyword search strategy with a proxy re-encryption scheme to protect user data security. This conjunctive keyword search method helps to search documents containing all of the requested keywords by using the conjunctive keyword. It allows users to search for several terms at once [8].

II. Related Works

Abdur et al., [1] suggested a mobile edge computing framework that can provide real-time and location-aware customized services to a big crowd. At the server end, the architecture employs a combination of cloud and Fog Computing Terminals (FCT) at the crowd edges and also builds the infrastructure to provide context-aware services for the millions of pilgrims that congregate each year in a tiny region area.

Dan et al., [2] presented the idea and characteristics of edge computing on a set of criteria for secured data analytics using edge computing by examining possible security concerns. Furthermore, edge computing can provide a complete assessment of the pros and cons of existing researches on data analytics in edge computing.

Traffic and Energy Saving Encrypted Search (TEES), a bandwidth and energy efficient encryption search paradigm over mobile cloud is suggested by Jia et al., [4]. In this work, architecture enhances communication between mobile clients as well as the cloud by offloading computing from mobile systems to the cloud. It is also shown that when performance enhancement methods are used, data privacy does not suffer.

On encoded smart body sensor network data, Lan et al., [5] presented a Memory Leakage-Resistant Dynamic and Verifiable Multi keyword Ranked Search system (MLR-DVMRS). To achieve memory leakage resistance, the unclonable approach utilized by fuzzy extractors.

Lili et al., [7] presented a privacy-preserving conjunctive keyword search scheme over encrypted cloud data that allows dynamic updating operations and at the same time, also introduced Multi-attribute Conjunctive Keyword Search strategy based on Multi-Attribute Tree (MCKS-MAT) method that can accomplish equality, subset and range conjunction while also satisfying privacy and security requirements under the recognized background attack scenario.

SSE (Searchable Symmetric Encryption) and PEKS (Public Key Encryption with Keyword Search) are the two primary methods of Symmetric Encryption, according to Wang et al., [8]. This article categorizes and compares several Symmetric Encryption systems in terms of usefulness, efficiency and security. Further, it identifies some promising new areas for research on Symmetric Encryption systems.

Yin et al., [9] discussed the fundamental attacks and influential assaults. In this research, defensive mechanism is applied to edge computing systems to better understand the threats and problems of securing these systems.

III. Methodology

The following approaches are developed to overcome the constraints of present methodology.

A. Time Domain Multi-Authority Outsourcing (TMO)

To improve data security and safeguard user privacy, Time Domain Multi-Authority Outsourcing uses an attribute-based encryption technique. Time Domain Multi-Authority Outsourcing, in particular includes time as one of the encrypting factors and divides attributes into universal and temporal attributes, allowing more flexible data access method. It expanded their multi-authority attribute-based encryption approach by exporting decryption to edge nodes, which can significantly may cost low. Time Domain Multi-Authority Outsourcing also has an easy-to-use approach for changing access policies. Edge storage nodes can update the access policy of the existing ciphertext online without wasting network traffic, rather than requiring the data owner to obtain the encrypted data and decrypt it for further distribution.

In the edge computing environment, a time domain outsourced multi-authority attribute-based encryption technique is used. For data gathering and exchange, Time Domain Multi-Authority

Outsourcing enables safe and efficient fine-grained access permissions. Time is a deterministic element for data use with ever-increasing data and advanced applications. To maintain security and system adaptability it is necessary to incorporate time domain information within the encryption scheme. Time Domain Multi-Authority Outsourcing also makes use of the advantages of edge computing to provide multi-authority and outsourcing characteristics in order to boost efficiency. The security concern posed by key ciphertext communication between both the cloud and the terminal is also reduced by outsourcing to edge nodes. Plain data are divided into data blocks, which are then encrypted locally with symmetric encryption and also the multi-authority attribute-based encryption technique is used to encrypt the encryption key. Edge Storage Node (ESN) receives both forms of ciphertext for storage. Universal attributes and temporal attributes make up Time Domain Multi-Authority Outsourcing attributes. The private keys for legal data users are correct and their accessing time is likewise within the acceptable time period. Further by delivering the matching modified edge key, data consumers can utilize Edge Computing Node (ECN) to pre-decrypt the ciphertext. Finally, after executing the minimal decryption locally, users get the data content.

B. Online/Offline Multi-Authority Decryption Outsourcing (OOMADO)

Data Owner (DO) is an entity to hold data and encrypts it before uploading it to cloud servers. A data owner does not want the Cloud Service Provider to understand anything about the data and permits access to data users whose attributes match a particular policy. Data owners may be forced to encrypt their data using resource-constrained devices while the gadgets remain reliable.

The Cloud Service Provider (CSP) provides storage space to data owners. Thought the Cloud Service Provider is a stranger and tries to extract information from data it has and the data cannot be changed or removed. Data Users (DU) seek to see data that the owner has outsourced to the Cloud Service Provider and get access to this information after meeting certain criteria. Attribute Authorities provided the data users with decryption keys corresponding to their attributes but the users of data become untrustworthy and attempt to obtain unauthorized data. Hence, it is important for Attribute Authority and data users to work together. Each data user is assigned a Global Identification (GID), such as a social security card or a passport number, which must be provided to the attribute authorities in order to acquire the decryption keys. All decryption devices used by Data Users are assumed to be trustworthy but there is more Attribute Authorities (AA) to manage distinct user attributes and create the matching public key and decryption key.

On providing global IDs, data users get their attributes and accompanying decryption keys from appropriate attribute authorities global identifiers (GID). For instance, the department of Motor Vehicles might be an Attribute Authorities (AA) and recognizes that a certain data user is capable of driving. A university may also verify a data user as a student of institution but it is possible that certain Attribute Authorities (AAs) are corrupted. Proxy Server (PS) executes partial decryption of the encrypted cypher text for data user after receiving a modified decryption key from data user. This system reduces the decryption load on user devices while keeping the proxy server known about the encrypted traffic. The proxy server may attempt to extract as much data as possible from ciphertext, but this has no effect on the transformation validity. It might be a component of cloud server or perhaps an independent entity. The system parameters are defined by the System Manager (SM). Hence the data user needs to upload the authentication of data using the attribute-based multi-authority ciphertext encryption system online/offline cryptographic techniques.

C. Proposed Methodology

The results of the proposed scheme are presented and algorithms are discussed. The three steps of the proposed scheme. The initial step is global set up of the entire process. By establishing and distributing global parameters to data owner and edge server, user initiates process of the system. If the user wants to access the server requested data files the user need to have authentication from the data owner. The data owner further authenticates user upon receiving the request and then creates the private key using the valid trapdoor. The next step is that the data owner carries out the performs immediately after authenticating the user. The authorized person encrypts the documents as well as the index, which comprises a list of keywords. Then owner uses the private key to publish the encrypted documents and index to the edge server. The data owner additionally specifies the time period for each user with a beginning (day/month/year) and end (day/ month/ year) pattern. While the data owner updates files to the edge server, the data user is allowed to search documents using keywords. This feature proposed in the system allows the user to do a search at any moment of time. When the effective time expires, the users search authority is automatically revoked. The current time information is encoded in the re-encrypted cipher text with a time seal in order to achieve the time controlled access right revocation. The user requests the server at a specific time using the time sealer and the request is denied if the time information buried in the re-encrypted cipher text differs from the time supplied by the owner. By providing separate time seals, the data owner can give different time periods for different consumers. Because the limitation is created, the owner is bound by the effective time period. It maintains record of previously searched documents containing keywords as a local filter within that edge server. Every previously searched data are saved in cipher text format in the filter and this allows users to quickly and easily locate the documents. Because the attribute-based conjunctive keyword search scheme is used, the user is aided by the fact that all sought terms are included in the required documents. This minimizes user workload by reducing the quantity of documents. In the last step, the user uses an attribute-based conjunctive term with the trapdoor to query the edge server and the server replies to the search query when the time seal contained in the trapdoor meets the effective time private key as well as time seal T period embedded in the proxy re-encrypted ciphertext. Instead, if the edge server denies the search request, the edge server becomes a proxy to re-encrypt the cipher text that fits the keyword after checking the time period. Unless the user gets permission, the edge server goes through a re-encryption process with a fresh key and this process does not take place otherwise. As a result, both computational complexity and time delay are reduced. Because the data owner offers various time for different users, the proposed scheme is intended to enable multi-users.

Social engineering is the use of shareable information to allow attackers to transmit fraudulent payments in the name of the particular recipient. The same data are sold in the open market for a profit and used to track down the original users identity. Due to their user satisfaction and simplicity of access, mobile wallets achieve maximum use through widespread user participation. Many new policy initiatives are predicted to be in place to keep the security protocols such as authentication, authorization, integrity, confidentiality and privacy in area when it comes to sensitive information stored in the mobile wallet. Some of the most new advancements that need to be examined and implemented provide mobile wallets an extra support.

Encryption is the process of converting textual information into an unreadable message. This encryption is essential in e-wallets to ensure their validity. Privacy is defined as the access to personal data and the desired access over unauthorized use. To establish the validity and increase the privacy of network transactions, every stated wallets use a unique encryption technique. The types of keys utilized, access control, the security method employed and the quantity of bytes of input data are the all elements in the encryption technique process.

Encryption appears to be one of the best data security techniques available today. Data security is improved by user authentication and transparent encryption. Attacks on data or information transferred via a mobile device can be avoided. Because there are so many vulnerabilities to access data, attackers role gets more relaxed in gaining access to all personal information.

In traditional web wallet, the information is needed to be supplied online but susceptible to phishing attacks, compromising data privacy. The ultimate objective of every security mechanism is to enable lawful access to mobile devices and upcoming transaction to be done through applications. It discusses several encryption techniques and benefits for use in mobile wallet applications.

The user with a secret key encrypts using such a public key and decodes with a secret key while maintaining a certain level of confidentiality. The attributes are used to represent user credentials and now the user who encrypts a communication establishes a unique password for the recipient who decrypts it. The encrypted data in Cipher Text Attribute Based Encryption (CPABE) remains private and protected against collusion attacks. Encryption is performed using a set of attributes provided by the authorities and random numbers, whereas decryption is performed if the decrypting entity provides at least x number of attributes.

Unified Payment Interface (UPI) is a significant factor that allows users to make payments directly from bank accounts using their e-wallet. In the recent years, millions have been utilizing the e-wallet, but it has its own set of constraints. Compatibility is one of the restrictions. Initially, the money transfer between the sender and the receiver has been made from same bank account but now it is almost a constraint that money could not be transferred from wallet to bank. Strategies to resolve interoperability via UPI, as well as robust security in all e-wallets can be created in the future. In order to ensure the security of the payment channel and payment mode, sessions during the time it takes to get One Time Password (OTP) in wallets should be secured.

E-wallet apps made it especially simple for users to do transactions easily and frequently. Too many business sectors have adopted the widely used notion of an e-wallet, each with their own flavour and set of features. However, there are still enough security issues. The different security threats leaks have been explored in this work and stronger wallets have been developed. A new fresh type of e-wallet application can be created by taking into account the problems that need to be addressed.

The proposed scheme is built utilizing the NS2 simulator. To implement experimental work, the performance evaluation of proposed technique with number of mobile users is examined. The proposed scheme is performed with different numbers of data and measured with different parameters. The analysis of proposed scheme is compared with the existing TMO, OOMADO, Bayesian Method and Game Method performance.

IV. Experimentation and Results

The development of mobile network access and mobile wallets, also known as e-wallets have become one of the most commonly used platforms for making payments under financial regulations from a mobile device. It has spread to all corners of the globe and is utilized by common people although due to its easiness of use and utility. In recent years, the growth of mobile wallets has been tremendous with programmes like as Paytm, Paymate, PayUmoney, MobiKwik and others thus making it easier for users to manage and make secured payments.

E-wallets have replaced traditional wallets by lowering the use of cash amongst people. According to research findings, cashless transactions are simple to use and save time, but security is still a risk. Mobile wallet apps rely on insufficient resources such as restricted battery life, bandwidth, storage space and processing performance. By offloading computations to a resourceful server, such restrictions can be greatly alleviated.

Large-scale simulations are not permitted in this environment. Outsourced validation of the computations is now delegated to an untrustworthy server. It is clear that even when payments are made over wireless networks, a wide range of security challenges such as denial of service, rogue access points and security attacks are feasible. The consumer requires transaction information, such as credit and debit card numbers while the edge server authenticates or verifies the customer after receiving a response from the customer and generates a secured private key with authorized trapdoor. Further the edge server then encrypts the information and creates an index for easy retrieval. The index in this scenario is much more than a collection of unique keywords, such as an account number or a customer name and encrypts the document before uploading and indexing it to the edge server using the secure private key. In addition, the edge server specifies a time period for each users and the time sealer specifies the time period.

The customer uses the conjunctive keywords with trapdoor to request data from edge server. The time embedded as in data at the time sealer then must match the customer request time. If the time period is the same, the edge server serves as a proxy server, re-encrypting the cipher text with a fresh private key. The re-encryption procedure is only done when the customer has been granted approval. Finally, the customer receives the re-encrypted cipher text with fresh private key for decryption from edge server. To enhance search efficiency, a local filter maintains record of earlier document access.

To assess the proposed scheme performance, characteristics such as computing overload, encryption time and decryption time are compared to existing methods such as Time Domain Multi-Authority Outsourcing (TMO) and Online/Offline Multi-Authority Decryption Outsourcing (OOMADO).

4.1 Performance Analysis of Computational Overhead

The analysis of proposed scheme is compared with existing TMO, OOMADO, Bayesian Method and Game Method performance and is shown in Table 1.1.

Table 1.1 Impact of Computational Overhead

Total no. of Mobile Users	Existing Bayesian Method	Existing Game Method	Existing TMO	Existing OOMADO	Proposed Scheme
10	50	44	11	13	9
20	39	31	21	26	11
30	58	47	33	36	24
40	78	65	40	75	33
50	96	73	45	80	38

It represents the variation of computational overhead time with the system time of existing methods.

4.2 Performance Analysis of Encryption Time

The evaluation of proposed scheme is compared with existing TMO, OOMADO, Bayesian Method and Game Method and is given in Table 1.2.

Table 1.2 Impact of Encryption Time

No. of Attributes Authorities (AA)	Existing Bayesian Method	Existing Game Method	Existing TMO	Existing OOMADO	Proposed Scheme
2	4300	3600	1100	1600	1000
4	3100	3017	2000	2200	1800
8	2620	2518	2500	2800	1900
10	5140	4198	3800	4000	2800
12	8750	7412	4800	7000	4000

The variation of computational overhead time with the system time of existing schemes.

4.3 Performance Analysis of Decryption Time

The performance of proposed scheme is compared and evaluated with existing TMO, OOMADO, Bayesian Method and Game Method and is presented in Table 1.3.

Table 1.3 Impact of Decryption Time

No. of Attributes Authorities (AA)	Existing Bayesian Method	Existing Game Method	Existing TMO	Existing OOMADO	Proposed Scheme
7	295	135	25	15	12
10	318	180	38	22	19
15	452	174	45	36	28
25	580	289	58	42	38
33	242	112	72	53	45

The variation of decryption time with the system time of existing methods.

4.4 Performance Analysis of Search Efficiency

The search efficiency of proposed scheme is compared with TMO, OOMADO, Bayesian Method and Game Method. It is shown in Table 1.4.

Table 1.4 Impact of Search Efficiency

No. of Attributes Authorities (AA)	Existing Bayesian Method	Existing Game Method	Existing TMO	Existing OOMADO	Proposed Scheme
20	9.5	8.1	7.5	3.5	2.5
40	13.8	12.0	9.8	3.6	2.0
60	25.2	17.4	4.5	3.9	2.4
80	30.5	26.9	5.8	4.0	2.1
100	24.2	21.7	7.2	3.5	1.8

It represents the measures of search time when compared with number of keyword-document pairs for existing schemes TMO, OOMADO, Bayesian Method and Game Method. Attribute based conjunctive keyword search Encryption scheme is used in proposed scheme in order to evaluate the Search Efficiency. The search efficiency is found to be higher for the proposed scheme when compared to TMO, OOMADO, Bayesian Method and Game Method.

V. CONCLUSION

The growing popularity of the Internet of Things (IoT), trend towards combining traditional cloud computing with resources available at the edge of the network. This way it becomes possible to exploit the complementary characteristics of both types of platforms. However, unifying the two types of platforms poses new challenges to developers and operational becomes increasingly harder to determine where services should run based on their non-functional and runtime-requirements, while simultaneously utilizing the resources at hand in an optimal way. The proposed attribute-based conjunctive keyword search scheme is developed and coupled with a proxy re-encryption technique to safeguard users data. Additionally, the amount of time allotted to each client in order to decrease user complexity. The proposed scheme is 10% more efficient than existing methods in terms of safeguarding data and protecting the privacy of the owner. It comprised encryption, decryption and computational overhead process. The first work of proposed scheme is compared with the existing TMO, OOMADO, Bayesian Method and Game Method. As described in this research, the e-wallet applications implemented with proposed techniques are utilized effectively in edge computing.

REFERENCES

[1] Md. Abdur Rahman, ElhamHassanain, M. Shamim Hossain (2017), “Towards a Secure Mobile Edge Computing Framework for Hajj”, IEEE Access, Vol.5, Pp. 11768-11781.

[2] Dan Liu, Zheng Yan, Wenxiu Ding and Mohammed Atiquzzaman (2019),“A Survey on Secure Data Analytics in Edge Computing”, IEEE Internet of Things Journal, Vol.6, Iss.3, Pp.4946-4967.

[3] N. Hassan, K. A. Yau and C. Wu (2019), “Edge Computing in 5G: A Review”, IEEE Access, Vol.7, Pp.127276-127289.

[4] Jian Li, Ruhui Ma, Haibing Guan (2015), “TEES: An Efficient Search Scheme over Encrypted Data on Mobile Cloud”, IEEE Transactions on Cloud Computing, Pp. 2168-7161.

[5] Lanxiang Chen, Zhenchao Chen, Kim-Kwang Raymond Choo, Chin-Chen Chang, Hung-Min Sun (2018),“Memory Leakage-Resilient Dynamic and Verifiable Multi-Keyword Ranked Search on Encrypted Smart Body Sensor Network Data”,IEEE Sensors Journal,Vol.19,Iss.19,Pp.8468- 8478.

[6] Lili Zhang, Yuqing Zhang and Hua Ma (2018), “Privacy-Preserving and Dynamic Multi-Attribute Conjunctive Keyword Search Over Encrypted Cloud Data”, IEEE, Vol.6, Pp.2169-3536.

[7] Y.Li, F.Qi, Z.Wang, X.Yu and S.Shao (2020), “Distributed Edge Computing Offloading Algorithm Based on Deep Reinforcement Learning”, IEEE Access, Vol.8, Pp.85204-85215.

[8] Wang Yunling, Wang Jianfeng, Chen Xiaofeng (2016),“Secure searchable encryption: a survey”, Springer, Pp.52-65.

[9] Yinhao Xiao, Yizhen Jia, Chunchi Liu, Xiuzhen Cheng, Jiguo Yu and WeifengLv (2019), “Edge Computing Security: State of the Art and Challenges”, Proceedings of the IEEE, Vol.107, Iss.8, Pp.1608-1631.